


<p>CRIME PREVENTION & COMMUNITY RELATIONS</p>	 <p>YAVAPAI COUNTY <i>Arizona</i> SHERIFF'S OFFICE <i>Serving Since 1864</i></p>	<p>SCAMS & FRAUDS</p> <p>4 Pages</p>
255 East Gurley Street, Prescott AZ 86301	www.ycsoaz.gov	(928) 771-3260

Nigerian/West African Fraud

Watch out for the Nigerian/West-African Business letter scam! For years now, businesses, learning institutions, and government departments have been receiving e-mails from senders posing as Nigerian/West-African government or business officials offering to share large sums of money.

Do not become a victim. If you have received an unsolicited letter containing any of the characteristics listed below, you should carefully research available information before conducting a transaction. Most letters are variations of the following:

- You receive an "urgent" business proposal "in strictest confidence" from a Nigerian/West-African civil servant /businessman.
- The sender, often a member of the "contract review panel", obtained your name and profile through the Chamber of Commerce or the International Trade Commission.
- The sender recently intercepted or has been named beneficiary of the proceeds from real estate, oil products, over-invoiced contracts, cargo shipments, or other commodities, and needs a foreign partner to assist with laundering the money.
- Since their government/business position prohibits them from opening foreign bank accounts, senders ask you to deposit the sum, usually somewhere between \$25-50 million, into your personal account.
- For your assistance, you will receive between 15-30% of the total, which sits in the Central Bank of Nigeria awaiting transfer.
- To complete the transaction, they ask you to provide your bank name and address, your telephone and fax numbers, the name of your beneficiary, and, of course, your bank account numbers.
- The sender promises to forward your share within 10-14 working days!

Prize Pitch (Lottery) Scams

The classic prize pitch scam involves victims receiving notification by mail, phone, or e-mail indicating they have won a prize (monetary or other valued item).

However, in order to collect the prize the victim is required to pay various fees or taxes in advance. Victims either never hear from the organization again or receive further requests for money.

Tips

- Keep track of contests, draws and lotteries you enter.
- Challenge a caller who says you've won a prize to tell you where and when you entered.
- If you didn't enter, you can't win.

Watch out for charity scams

Since fraud artists hope to profit from people's generosity, the Sheriff's Office would like to remind you to be wary of false charity scams. Consider the following precautions to make sure your donations benefit the people and organizations you want to assist:

- Be wary of appeals that tug at your heart strings, especially pleas involving current events.
- Ask for written information about the charity, including name, address and telephone number. A legitimate charity or fund-raiser will give you information about the charity's mission, how your donation will be used and proof that your contribution is tax deductible.
- Ask the solicitor for the registered charitable tax number of the charity. Question any discrepancies.
- Check out the charity's financial information. For many organizations, this information can be found online.
- Ask for identification. If the solicitor refuses to tell you or does not have some form or verifiable identification, hang up or close the door and report it to law enforcement officials.
- Call the charity. Find out if the organization is aware of the solicitation and has authorized the use of its name. If not, you may be dealing with a scam artist.
- Watch out for similar sounding names. Some phony charities use names that closely resemble those of respected, legitimate organizations. If you notice a small difference from the name of the charity you intend to deal with, call the organization to check it out.
- Be skeptical if someone thanks you for a pledge you don't remember making. If you have any doubts about whether you've made a pledge or previously contributed, check your records. Be on the alert for invoices claiming you've made a pledge. Some unscrupulous solicitors use this approach to get your money.
- Refuse high pressure appeals. Legitimate fund-raisers won't push you to give on the spot.
- Be wary of charities offering to send a courier or overnight delivery service to collect your donation immediately.
- Be wary of guaranteed sweepstakes winnings in exchange for a contribution. According to law, you never have to donate anything to be eligible to win.
- Avoid cash gifts. Cash can be lost or stolen. For security and tax record purposes, it's best to pay by check.

Advance Fee Fraud

Classified advertisements for loan opportunities do not guarantee the legitimacy of a company. Some companies claim they can guarantee you a loan even if you have a bad credit history or no credit-rating at all. They usually request an up-front fee of several hundred dollars. If you send your money to these companies, it is unlikely you will get your promised loan and your advance payment will be at risk.

Advance fee loans operating for a criminal purpose generate millions of dollars annually in the U.S. Persons with poor credit ratings are usually the key targets and once the 'loan processors' receive your money, they usually disappear.

Tip

- If you have doubts about the organization, contact the [Better Business Bureau](#) for further information

E-mail Fraud / Phishing

Recognize it

What is Phishing?

Phishing is a general term for e-mails, text messages and websites fabricated and sent by criminals and designed to look like they come from well-known and trusted businesses, financial institutions and government agencies in an attempt to collect personal, financial and sensitive information. It's also known as brand spoofing.

Facts

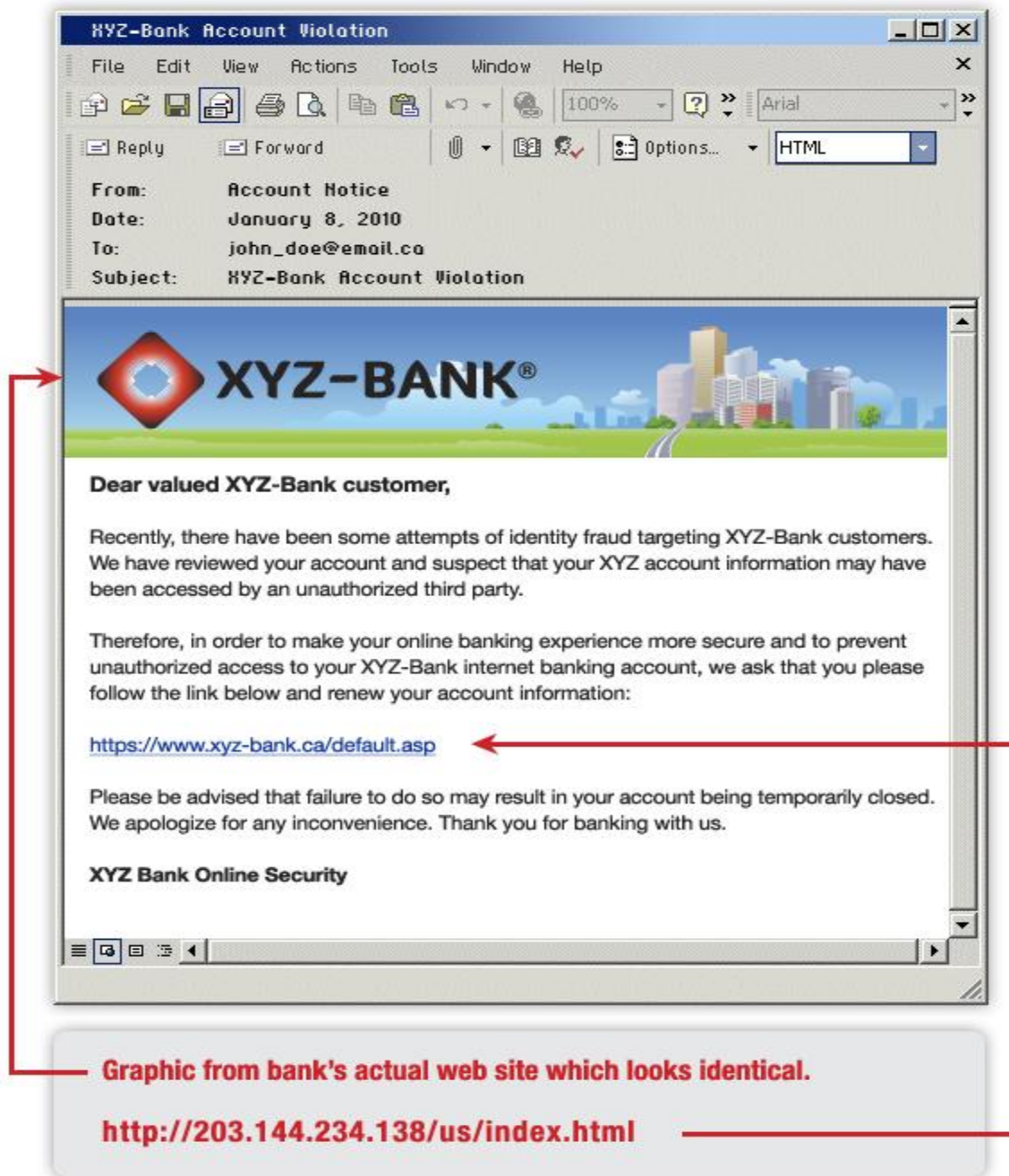
Characteristics

- The content of a phishing e-mail or text message is intended to trigger a quick reaction from you. It can use upsetting or exciting information, demand an urgent response or employ a false pretense or statement. Phishing messages are normally not personalized.
- Typically, phishing messages will ask you to "update," "validate," or "confirm" your account information or face dire consequences. They might even ask you to make a phone call.
- Often, the message or website includes official-looking logos and other identifying information taken directly from legitimate websites. Government, financial institutions and online payment services are common targets of brand spoofing.

Catch phrases:

- *E-mail Money Transfer Alert: Please verify this payment information below...*
- *It has come to our attention that your online banking profile needs to be updated as part of our continuous efforts to protect your account and reduce instances of fraud...*
- *Dear Online Account Holder, Access To Your Account Is Currently Unavailable...*
- *Important Service Announcement from..., You have 1 unread Security Message!*
- *We regret to inform you that we had to lock your bank account access. Call (telephone number) to restore your bank account.*

Example of a Phishing E-mail



In some cases, the offending site can modify your browser address bar to make it look legitimate, including the web address of the real site and a secure "https://" prefix.

Information sought: Social Security numbers, full name, date of birth, full address, mother's maiden name, username and password of online services, driver's license number, personal identification numbers (PIN), credit card information (numbers, expiry dates and the last three digits printed on the signature panel) and bank account numbers.

What your information could be used for: Phishing criminals can access your financial accounts, open new bank accounts, transfer bank balances, apply for loans, credit cards and other goods/services, make purchases, access your personal email account, hide criminal activities, receive government benefits or obtain a passport.